



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,409	04/01/2004	Huw Edward Oliver	300203614-2	7989
7590 HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			EXAMINER CHERY, DADY	
		ART UNIT 2616		PAPER NUMBER
			MAIL DATE 08/06/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/815,409	OLIVER ET AL.
	Examiner	Art Unit
	Dady Chery	2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) Responsive to communication(s) filed on 04/01/2004.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) Claim(s) 1-39 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-39 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date 06/12/2007.

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Claim Objections***

1. Claim 19 is objected to because of the following informalities: Claim 19 depends on claim 17 and refers to a data storage, but there is no storage data in claim 17. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 101***

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. "a data storage media comprising program" is not being executed by a computer. This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Data storage does not fall within a statutory category since it is clearly not a series of steps or acts to constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substances to constitute a composition of matter.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1,2,4-12,14-28, 30,31,32 rejected under 35 U.S.C. 103(a) as being unpatentable over Yeager et al. (US Patent 7,213,047, hereinafter Yeager) in the view of Gleichauf et al. (US Patent 7,137,145, hereinafter Gleichauf).

Regarding claims 1 and 27, Yeager discloses a *method of operating a computer entity in a network of computer entities that communicate with each other on a peer-to-peer basis* (Fig. 1B), *the method comprising operating a reputation management process for managing at least one other said computer entity of the network* (Fig. 47, Col. 35, lines 40 - 46); *the management process comprising*:

(a) *collecting a plurality of reputation data items, each reputation data item describing an aspect of operation of a said at least one other computer entity of said network* (Col. 34, lines 56 – 58 and Col. 35, lines 40 – 46);

(b) *monitoring said plurality of reputation data items* (Col. 39, lines 9 – 10);

Yeager fails to teach

(c) *generating an alert message in response to changes in at least one said reputation data item.*

However, Gleichauf teaches a method of generating a signal when an infective element is detected in network (Col. 1, lines 42 – 50). Which is considered substantially as the same function of the instant application.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a signal when there is a change in network for the purpose of disabled an infected element.

Regarding claims 2 and 12, Yeager discloses all the limitation of claim as applied above except *the method of multi-casting said alert message to a plurality of other said computer entities.*

However, Gleichauf teaches *the method of multi-casting said alert message to a plurality of other said computer entities* (Col. 2, lines 22 – 35).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to broadcast the alert message to a plurality of other said computer entities in order to allow quick identification of an infective element (Col. 2, lines 33 –35).

6. Claim 3, 13,36 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yeager in the view of Gleichauf as applied to claim 1 above, and further in view of Implementing a Reputation -Aware Gnutella Servent by Cornelli et al. (hereinafter Cornelli).

Regarding claim 3, 13,36 and 39, Yeager discloses all the limitations of claim 3 except *the method of applying a voting protocol to determine a group action on usage of said at least one other said computer entity.*

However, Cornelli teaches a method of applying a voting protocol to determine a trustable entity (Page 7, lines 1 –7). Which is considered substantially as the function as the instant application.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a voting protocol to determine the credibility of an agent (Page 7, lines 7 –8).

Regarding claims 4, 14, 23,24, 31 and 32, Yeager discloses *the method of determining changes in performance of said at least one other computer entity from changes in said reputation data items* (Col.39, lines 11 – 15). Where the forming of new groups according to the results of the analyzing data is considered as the same function described by the instant application.

Regarding claims 5, 15, 19, 22 and 30, Yeager discloses *the method of sensing abrupt changes of a said aspect of operation of a said at least one other computer entity whereby to determine the possible existence of a technical operating problem with that entity, and outputting an alert message indicating this possible technical operating problem* (Col. 2, lines 64 – Col. 3, lines 8). Where the unavailability of the peer node is considered as an abrupt change and a technical operation problem.

Regarding claim 6, Yeager disclose *the method of said reputation data is collected from a plurality of peer computer entities, which are operable to access said at least one other computer entity of which said changes in performance are sensed* (Col. 2, lines 44 –47, and Col. 39, lines 11 –16).

Regarding claims 7, 21 , 28, 34 Yeager discloses wherein *the reputation data items have types selected from the set* (Col. 3, lines 9 –30):

*a satisfaction data describing whether a user of a computer entity of said network is satisfied with their experience of said at least one other computer entity, or is not satisfied* (Col. 3, lines 13 – 21); Where the trust evaluation is considered a satisfaction data

*a found/not found data describing whether a user of a computer entity of said network found a service at a particular said at least one other computer entity or did not find said services at said particular said at least one other computer entity* (Col. 2, lines 65 – Col. 3, lines 5); Where the unavailability of the peer resources is considered as “a found/not found data” as described by the instant application.

*an ease of use data describing whether a user found a specified computer entity to be easy to use or to be difficult to use* (Col. 2, lines 52 –64). Where the size of the payload is considered as an ease of use data.

*a service provision data describing whether a computer entity is capable of providing a service or resource, to a user requesting said service or resource, or whether said computer entity is incapable of providing said service or resource* (Col. 2, lines 44 – 51).

Regarding claim 8 Yeager discloses the step (a) comprises *storing reputation data in a database locally at said computer entity, said reputation data describing at least one reputation data type for each of one or a plurality of other computer entities of said network* (Col. 30, lines 10 –13 and Col.38, lines 17 –19); and step (b) comprises

*analyzing said reputation data to determine a performance parameter of at least one said computer entity (Col. 39, lines 9 –15).*

Regarding claim 9, Yeager discloses *the reputation data items provide reputation data describing a plurality of user experiences of one or a plurality of other computer entities of said network* (Col. 2, lines 4 – 13), *step (c) comprising generating a set of alert messages dependant upon a reputation data collected in step (a)* (Col. 30, lines 25 – 27 and Col. 31, lines 36 –40). Where the indicating message is considered as an alert message.

Regarding claims 10, 25, 26 Yeager discloses *the method of determining whether to interact with said at least one other computer entity on the basis of reputation data derived from the reputation data items collected in respect of said at least one other computer entity* (Col. 2, lines 34 – 38). Where the relevant interest is considered as the same function of the instant application.

Regarding claim 11, Yeager discloses a computer entity (Fig. 1B) comprising: *a computer platform capable of providing a set of resources including communication resources for communicating with other computer entities on a peer-to-peer basis* (Col. 3, lines 31 – 40); *a reputation service component capable of providing a reputation service for monitoring quality of service parameters of at least one said other computer entity* (Col. 3, lines 9 – 18);

said reputation service component being arranged to:

*collect a plurality of reputation data items each describing an aspect of operation of a said at least one other computer entity* (Col.34, lines 56 – 58 and Col. 35, lines 40 – 46);

Yeager fails to teach

(c) *generating an alert message in response to changes in at least one said reputation data item.*

However, Gleichauf teaches a method of generating a signal when an infective element is detected in network (Col. 1, lines 42 – 50). Which is considered substantially as the same function of the instant application.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a signal when there is a change in network for the purpose of disabled an infected element.

Regarding claim 16, Yeager discloses *the computer entity wherein the reputation service component further comprises at least one analysis component* (Fig. 51, 510) *for analyzing a reputation data item.*

Regarding claim 17, Yeager discloses *the computer entity wherein the reputation service component is arranged to collect reputation data items from a plurality of computer entities in a peer to peer network* (Fig. 50A, 51); *the reputation service component being further arranged* (Col. 39, lines 50 –55):

*to analyze the reputation data items and, as a result of this analysis, to identify changes in reputation for individual ones of said other computer entities* (Col. 39, lines 54 –58);

*to generate a reputation message upon identifying a significant change in reputation, said reputation message describing a reputation of said at least one other computer entity* (Col. 39, lines 64 –68);

*to send said reputation message to at least one other computer entity of said network* (Col. 40, lines 44- 46).

Regarding claim 18, Yeager discloses a data storage medium storing program data (Fig. 34, 1302) for operating a computer entity in a network of computer entities, said program data comprising instructions for causing said computer entity (Col. 6, lines 54 – 64) to:

*operate a peer-to-peer protocol for communicating with other computer entities of said network* (Col. 2, lines 29 –35);

*perform a management process for management of at least one other said computer entity of said network*(Col. 35, lines 33- 36), said management process comprising:

*collecting a plurality of reputation data items, each reputation data item describing an aspect of operation of a said at least one other computer entity of said network* (Col.34, lines 56 – 58 and Col. 35, lines 40 – 46);

*monitoring said plurality of reputation data items*(Col. 39, lines 9 –10);

Yeager fails to teach

(c) *generating an alert message in response to changes in at least one said reputation data item.*

However, Gleichauf teaches a method of generating a signal when an infective element is detected in network (Col. 1, lines 42 – 50). Which is considered substantially as the same function of the instant application.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a signal when there is a change in network for the purpose of disabled an infected element.

Regarding claim 20, Yeager discloses a *method of operating a plurality of computer entities in a computer network* (Fig. 1), *said plurality of computer entities interacting on a peer to peer basis* (Fig. 47, Col. 35, lines 40 - 46); the method comprising:

*each said computer entity operating a peer to peer protocol allowing the computer entity to interact with at least one other said computer entity of said network* (Col. 2, lines 29 –35);

*at least one said computer entity of said network performing a management process comprising collecting reputation data from at least one other said computer entity of said network* (Col. 35, lines 33- 36) *said reputation data describing at least, one users perception of a performance parameter of one or more said computer entities of said network* (Col.34, lines 56 – 58 and Col. 35, lines 40 – 46);

Regarding claim 26, Yeager disclose *the method, wherein said management process comprises determining whether or not to interact with a said computer entity of said network, based upon said reputation data collected from said at least one other computer entity* (Col. 3, lines 17). Where the unreliability consideration is considered as the same function of the instant application.

Regarding claim 29, Yeager discloses a computer entity adapted for communication on a peer-to-peer basis with other computer entities (Fig. 1B) and comprising:

*a data collection arrangement for collecting reputation data (Fig. 50A,500A) from a plurality of computer entities in a peer to peer network, the reputation data collected from each entity of said plurality describing a user's perception of a performance parameter of one or more other computer entities of said network* (Col. 39, lines 50 – 56);

*an analysis arrangement for analyzing (Fig. 51, 510) said reputation data to identify changes in reputation data for individual ones of said other computer entities* (Col. 39, lines 56 – Col. 40, lines 4);

Yeager fails to teach a message generation arrangement arranged to respond to the identification arrangement identifying a significant change in reputation data, by generating a reputation message describing a reputation of said at least one other computer entity; and an output arrangement for sending said reputation message to at least one other computer entity of said network.

However, Gleichauf teaches a *message generation arrangement* (Fig. 1,42) arranged to respond to the *identification arrangement identifying a significant change in reputation data*, by generating a *reputation message describing a reputation of said at least one other computer entity*; and an *output arrangement for sending said reputation message to at least one other computer entity of said network* (Col. 9, lines 47 –56).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Gleichauf into the teaching of Yeager for the purpose of detect and disable an infective peer in the network (Abstract).

7. Claims 33,35,38 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yeager et al. in the view of Cornelli.

Regarding claim 33, Yeager discloses a *method of operating a computer entity in a network of computer entities that communicate with each other on a peer-to-peer basis* (Fig. 1B and Fig. 47, Col. 35, lines 40 - 46); said method comprising:

*collecting reputation data about at least one other computer entity in said network* (Col.34, lines 56 – 58 and Col. 35, lines 40 – 46);

*monitoring said reputation data to detect changes in performance of said at least one other computer entity* (Col. 39, lines 9 –10);

Yeager also discloses *broadcasting a message describing said reputation data, or changes in reputation data, to other peer computer entities in said network* (Col. 40, lines 44 –46); Where the propagation of the codat is considered as the same function of broadcasting a message describing the reputation data.

Yeager fails to teach the method of *applying a voting protocol to determine a group action of a plurality of peer computer entities in respect of said at least one other computer entity about which said reputation data has been collected.*

However, Cornelli teaches the method of *applying a voting protocol to determine a group action of a plurality of peer computer entities in respect of said at least one other computer entity about which said reputation data has been collected* (Page 7, lines 1 –7). Which is considered substantially as the function as the instant application.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a voting protocol to determine the credibility of an agent (Page 7, lines 7 –8).

Regarding claims 35 and 38, Yeager discloses *the reputation data about said at least one other computer entity is provided by at least one further computer entity of said network* (Col. 3, lines 9 –15).

Regarding claim 37, Yeager discloses a *computer entity adapted for communication on a peer-to-peer basis with other computer entities* (Fig. 1B) and comprising:

*a data collection arrangement* (Fig. 50A,500A) *for collecting reputation data about at least one other said computer entity* (Col. 39, lines 50 –56);

*a monitoring arrangement (Fig. 51, 510) for monitoring said reputation data to detect changes in performance of said at least one other computer entity (Col. 39, lines 56 – Col. 40, lines 4);*

*an output arrangement (Fig. 50A) for sending a message describing said reputation data, or changes in reputation data, to peer computer entities (Col. 40, lines 44 –46);*

*Yeager fails to teach a voting arrangement for causing a voting protocol to be applied to determine a group action of a plurality of peer computer entities in respect of said at least one other computer entity about which said reputation data has been collected.*

However, Cornelli teaches a voting arrangement (Fig. 2, poll) where the poll is considered as the voting arrangement *for causing a voting protocol to be applied to determine a group action of a plurality of peer computer entities in respect of said at least one other computer entity about which said reputation data has been collected* (Page 6, lines 18 – Page 7, lines 3).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a voting protocol to determine the credibility of an agent (Page 7, lines 7 –8).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dady Chery whose telephone number is 571-270-1207. The examiner can normally be reached on Monday - Thursday 8 am - 4 pm ESt.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ricky Q. Ngo can be reached on 571-272-3139. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dady Chery 08/02/2007

  
RICKY Q. NGO  
SUPERVISORY PATENT EXAMINER